移动 Agent 安全措施与实现①

林德树 黄廷磊 (桂林电子科技大学 计算机与控制学院 广西 桂林 541004)

摘 要： 移动 Agent 的应用日益广泛，移动 Agent 系统的安全问题突出，如何解决移动 Agent 安全问题是非常关键的。本文提出了基于密码学和计算机网络安全的移动 Agent 的安全措施，同时给出了实现的方法，并提出可以采用的其他新型的安全措施。这些措施的核心问题是既要保证移动 Agent 通信的安全和移动 Agent 执行环境的安全，同时又要保证移动 Agent 能够应用的更为广泛。

关键词： 移动 Agent; 安全; 加密; 信誉值

Mobile Agent Security Measures and Implementation

LIN De-Shu, HUANG Ting-Lei

(School of Computer and Control, GuiLin University of Electronic Technology, Guilin 541004, China)

Abstract: With the widespread application of mobile agents, mobile agent system's security is a prominent problem to be solved, and mobile agent's security question is critical. This paper proposes a mobile agent security architecture based on cryptography and computer network security. At the same time, the practical methods and suggested ways can be used in other new security measures. The purpose is for these measures do not only ensure the security of mobile agent communication and mobile agent execution environment, but at the same time ensure that this securidy system can be applied more widely to more mobile agents.

Keywords: mobile agent; security ; cryptography; reputation value

1 引言

移动 Agent(Mobile Agent 简称 MA)是 Agent 的一种，Agent 的研究起源于人工智能领域，Agent 是模拟人类行为与关系具有一定智能并能够自主运行和提供相应服务的程序。移动 Agent 是一个能够在异构网络中自主地从一台主机迁移到另外一台主机，并可与其他 Agent 或资源交互的程序[1]。移动 Agent 是分布式计算的重要组成部分。目前各种移动设备的上网过程中，网速和带宽都比较有限，这样就限制了移动网络的发展，移动 Agent 可以将请求 Agent 动态地移动到服务器端执行。而且有很多时候移动网络由于带宽的限制不能每时每刻都让各个移动网络设备同时在线，这样可以将用户提交的任务由移动 Agent 处理，在网络连接的时候再通过移动 Agent 访问网络和返回计算结果，就可以大大降低网络数据传送数据量，由于 Agent 是跨平台的，可以做到异构网络传输，扩大了移动 Agent 系统的使用范围。

随着电子商务的发展，移动 Agent 的研究日益频繁。在移动 Agent 中非常关键的是移动 Agent 应用安全措施的保障。在移动 Agent 应用系统中，核心问题是既要保证移动 Agent 通信的安全和移动 Agent 执行环境的安全，同时又要保证移动 Agent 能够应用的更为广泛。如果安全措施限制的太多，这样就使得移动 Agent 应用程序无法有效地在更大范围内移动，同时也限制了程序的普遍使用。如果安全措施不够就没有办法进行真正商用移动 Agent 软件的开发。

2 移动Agent安全措施结构图

移动 Agent 因为其在网络环境中运行，所以可能遇到很多网络攻击和欺骗。目前移动 Agent 系统中的主要安全问题主要体现在有两个方面[2]。

恶意 Agent 对目标主机的危害，恶意的 Agent

① 收稿时间:2010-01-22;收到修改稿时间:2010-03-29

移动到主机中窃取关键和重要信息，对系统够成威胁。

恶意服务主机对移动 Agent 的威胁，影响 Agent 的正常运行，干扰系统工作，窃取信息。

针对以上两个方面的问题，本文提出了具体解决方案。主要的安全措施有两个方面：

对移动 Agent 通信的关键数据和信息进行加密，并且移动 Agent 的通信环境可以根据安全要求，采用基于 SSL (Secure Socket Layer)协议的安全通信或者基于 VPN 的网络中实施移动 Agent 应用。

采用移动 Agent 安全信任模型 TMMARC[3],这个安全信任模型主要是对移动 Agent 体系中的各个实体采用信誉值评估，并且动态管理信誉值，依据信誉值作为通信的判断辅助依据。

综合以上要点，提出了移动 Agent 的安全措施框架结构如图 1 所示。

图 1　移动 Agent 的安全措施框架结构图

3　移动Agent通信安全措施

移动 Agent 通信安全措施可以利用加密算法和数字签名来解决。在基于 TCP/IP 协议通信网络中还可以利用 SSL(Secure Socket Layer)协议来保证网络安全传输数据。

3.1 采用 AES 加密的移动 Agent 安全措施

在移动 Agent 系统中的加密算法中可以采用 AES(Advanced Encryption Standard),这个算法又称作 Rijndael 加密法[4]。AES 是美国国家标准技术研究所 NIST 旨在取代 DES 而提出新的加密标准。AES 加密算法采用对称分组密码体制，密钥长度支持为 128、192、256，分组长度 128 位，算法应易于各种硬件和软件实现。

在这里我们可以根据不同的信息安全级别，采用不同长度的密钥来实现，如表 1 所示[5]。这里的分类不仅仅考虑数据的安全性要求，同时要考虑网络和实现的硬件代价，在实际的操作过程中我们把无线网络中的数据通信采用了 128 位密钥长度，这个主要是为了节省移动网络中的计算开销。

表 1　加密级别分类表

数据对安全性的要求	应用实例	密钥长度
较高	个人信息，银行数据，商业机密信息等	256
中等	联系方式，电话号码，住址	192
一般	无线网络信息，非私人信息	128
没有要求	例如：公共公布信息	可以不采用加密

3.2 通过 AES 加密算法的实现过程

AES 分组密码接受一个 128 位的明文，并且在一个 128，192，256 为密钥的控制下产生一个 128 位的密文。具体操作由称作轮(round)的步骤的集合，其中轮数可以为 9，11，13(取决于密钥长度)。一轮 AES 操作有 4 个步骤组成：1.SubBytes 2.ShiftRows 3.MixColumns 4.AddRoundKey[6]。

(1) SubBytes 函数

函数 SubBytes 步骤是 AES 算法中唯一利用非线性混合的步骤，这个操作是将 16 个字节的每一个都并行的映射为一个新的字节。一个 8 位二进制数据转换为另一个不同的 8 位二进制数据，这里要求一一对应，并且替换结果不能超出原来的位数，这个操作过程可以利用硬件和算法的方式来实现。SubBytes 函数执行如图 2 所示。

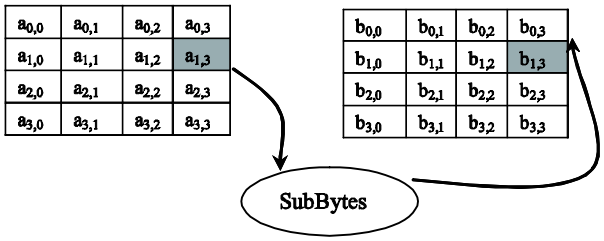

图 2　SubBytes 函数执行示意图

(2) ShiftRows 函数

ShiftRows 函数的功能是将状态数据中的每一行分别向右循环移动 0，1，2，3 位。这个状态变换比较容易实现。ShiftRows 函数执行如图 3 所示，其中

ROLi 代表循环右移 i 位。

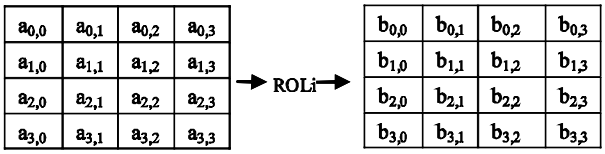

图 3　ShiftRows 函数执行示意图

(3)MixColumns 函数

MixColumns函数主要功能是对加密过程进行列变换，它的操作是将一个矩阵乘以状态矩阵的每一列得到新的矩阵中的一列，重复操作就得到了新的状态矩阵数据。MixColumns 函数执行如图 4 所示。

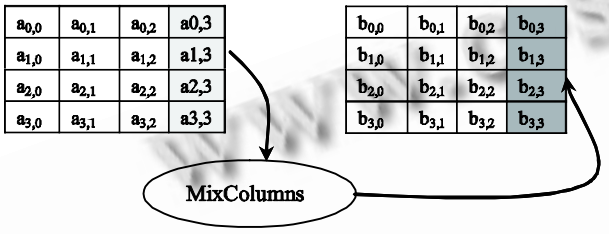

图 4　MixColumns 函数执行示意图

(4)AddRoundKey 函数

AddRoundKey 函数的功能是把密钥和状态数据进行异或得到新的状态数据，执行如图 5 所示。

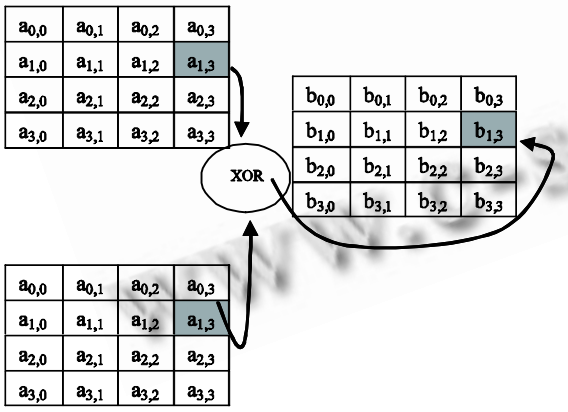

图 5　AddRoundKey 函数执行示意图

通过以上函数的多轮(9，11，13)执行就可以的到加密的数据，利用这样加密数据的传输虽然会耗费较大的计算代价，但是可以得到安全的数据。

3.3 移动 Agent 基于 SSL 通信

SSL 用以保障在 Internet 上数据传输的安全，利用数据加密(Encryption)技术，可确保数据在网络上传输过程中不会被截取及窃听。目前一般通用之规格为 40 bit 之安全标准，美国则已推出 128 bit 的更高安全标准。SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。所以在对安全性要求不高并且计算处理能力有限的网络应用中可以采用 SSL 协议通信。

3.4 移动 Agent 采用 AES 和 SSL 结合方式通信

对于数据安全性要求较高的移动 Agent 可以采用 AES 加密算法加密和 SSL 协议同时起作用。当然两者的结合方式要消耗很多的计算处理代价。

3.5 移动 Agent 运行环境安全措施

移动 Agent 运行的网络环境中有某些恶意主机，为了区分这些恶意主机，GhadaDerbas 提出了 TRUMMAR 模型,参考文献[3]中提出了安全信任模型 TMMARC[3],后者是对前者的改进。TMMARC 模型的主要思想就是对主机的安全信誉值进行评价，来评价哪些主机是安全的。确保通信只在安全的主机之间进行。

信任环境下移动 Agent 通信模型如图 6 所示，信任中心 TC1 有连个信任域。

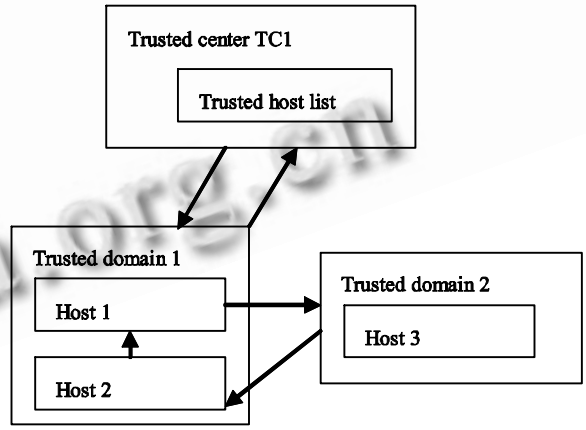

图 6　基于安全信誉的移动 Agent 通信模型

(1) 主机 1 首先查询本身的信任列表中是否有足够的信任主机来完成移动 Agent 任务，如果不够需要向信任中心获取信任主机。在这里主机 1 首先得到信任主机 2

(2) 如果信任主机 2 不能配合主机 1 完成移动 Agent 任务，主机 1 向信任中心查询信任主机列表，这项可以将信任域 2 中的主机 3 分配给主机 1

(3) 如果主机 1 选择主机 3 完成移动 Agent 任务，

这样主机 3 也同样要查询主机 1 是否在自己信任的主机列表中。如果在则接受完成执行移动 Agent，不在则不执行。这样可以确保整个通信环境都是在基于安全信誉之下进行操作。

3.6 实验结果

在移动 Agent 通信的过程中，我们分别采用了密钥的加密过程 128，192，256 位的实验，一共进行 10 次实验进行统计得到的统计数据如图 7。

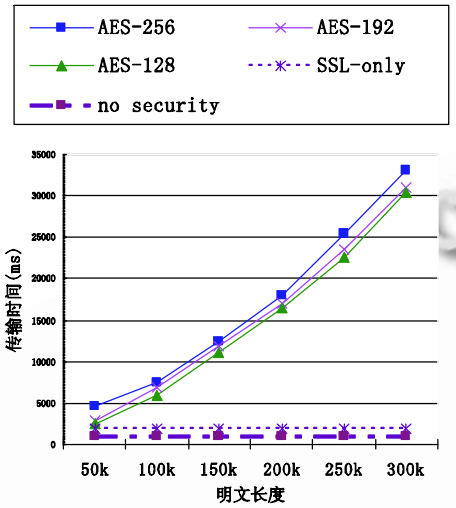

图 7　基于 Agent 通信时间消耗图

通过这个图我们可以对比发现，在没有加密措施的情况下采用 SSL 安全保障的时候系统消耗时间和不采用任何安全措相差不多，由于采用 AES 算法的时候，要通过加密，解密，哈希的过程消耗的计算时间较大，同时由于通过加密以后的密文数据基本是原来的 2 倍，所以这部分都的传输时间消耗更大，导致加密的时间比只是采用 AES 加密算法的传输时间增长。计算过程是采用发射返回式来测量时间。这样做要是为了防止通信双方的时间不同步，不利于计算通信时间。

4　其它安全措施

(1)　采用硬件方式来进行加密算法的计算

这种策略主要是为了减少移动Agent系统中的用于加密的计算时间，可以减轻处理加密数据的负担，提高系统的速度。在参考文献[7]中提出了这样的解决方案。

(2)　采用基于 VPN(rtual Private Network)的移动 Agent 传输

VPN 技术原是路由器具有的重要技术之一，在交换机，防火墙设备或操作系统软件里也都支持 VPN 功能，简单的说，VPN 的核心就是在利用公共网络建立虚拟私有网。由于 VPN 网络本身就具备很好的安全性，同时可以对可以扩展局域网络应用，所以利用 VPN 网络传输，不仅更安全，而且有利于移动 Agent 远程访问局域网资源。

除了以上提供的安全措施以外，随着移动 Agent 开发平台的进一步完善，目前也有很多移动开发平台已经考虑到移动 Agent 安全的问题，并且在系统中就集成了移动 Agent 安全的解决方案，这个当然更能够给移动 Agent 的安全问题的解决提供方便。

5　结束语

本文针对移动 Agent 安全问题，给出了移动 Agent 安全措施的具体解决方案。移动 Agent 安全措施的应用，关键的是要权衡移动性和安全性，在保证有较好的移动性的同时，能够充分利用软件算法或者硬件的方式来提高系统的安全性。移动 Agent 安全，涉及数据信息安全技术领域。本文提出的一种移动 Agent 安全访问的方法，实现了移动 Agent 访问信息的安全管理和认证，提高了移动 Agent 的安全性、灵活性和可维护性，并降低了系统的耦合度。这种安全措施的提出，扩大了移动 Agent 的使用范围。

参考文献

1 张云勇,刘锦德.移动 Agent 技术.北京:清华大学出版社, 2003.

2 丁建国,柳惠琳,陈涵生等.移动 Agent 的一种安全认证机制.计算机工程, 2001,2:74－75.

3 申永军,史小平,李小青.移动代理安全信任模型的研究.微计算机信息, 2009,25:39－41.

4 杨晓元,魏立线.计算机密码学.西安:西安交通大学出版社, 2007.

5 Sulaiman R, Sharma D, Ma WL. A Multi-Agent Security Architecture. 2009 Third International Conference on Network and System Security. 2009:184－191.

6 Denis TST, Johnson S.沈晓斌,译.程序员密码学.北京:机械工业出版社, 2007.

7 陈俊,王晶,曾晓洋等.低复杂度先进密码算法的 VLSI 实现.计算机工程,2007,33(4):143－145.